Security: online document sharing and storage

By Alex Walther, CPA, CFE, David Kirk, CPA/CFF, and Ryan Broussard

Recently on one of our engagements, an attorney's client requested they use Dropbox to transfer various data, documents, and information (the materials) between the various attorneys, experts (including forensic accountants), and company personnel. The attorneys agreed and their client proceeded to utilize a free third-party file sharing service to allow certain confidential items such as historical/projected financial statements, bank statements, and other confidential client documents to be accessed by all parties given authorization to access the materials. We recommended the attorneys use our secured file transfer (SFT) protocol Web site; however the attorney's client preferred to use the free third-party file sharing service.

As the matter proceeded, one of the attorneys asked if we knew about any potential risks that might exist when using the client's recommended free file sharing service. Our short answer was: it depends. There is not simply a yes /no answer; it depends on security requirements, the sensitivity of the materials and the facts and circumstances in the matter you are involved.

Managing confidential materials in a secure, safe way is one of the top priorities of forensic accountants who provide litigation support services and who must work with privileged and confidential materials daily. Using certain file sharing sites may open up users to unexpected risk when the materials are uploaded, downloaded, and/or stored with third-party services. In this article, we will discuss some items forensic accountants, attorneys and other professionals may want to consider.

How file sharing services work

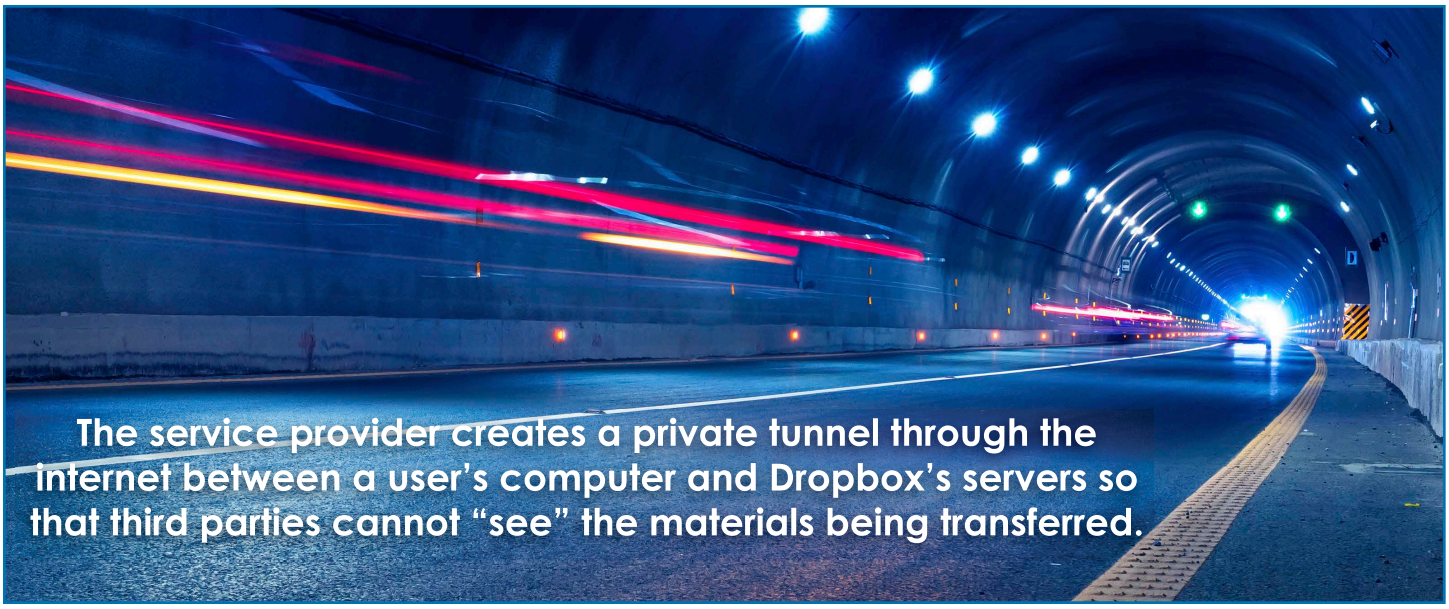
If you wanted to send a file (or a group of files) to another person, you could send it via e-mail(s) (depending on the size of each file), use a secured file transfer (SFT) Web site, or you could upload the files you wanted to share using a file sharing service that meets your security requirements. Utilizing a file sharing service entails uploading documents to the Internet, providing the intended recipient the means to access those same files, and the recipient accessing the files to view and/or downloading them to their computer. Dropbox, a well-known company in the file sharing service industry, describes its services as "a home for all your photos, docs, videos, and files…you can access your stuff from anywhere." Dropbox "also makes it super easy to share with others ..." Files uploaded to a file sharing site are then stored in the cloud (typically a server connected to the Internet) for future access or to share with others. Simplistically, file sharing sites allow a user to save information / data to the site's servers so that the user can access or provide others access to the material anywhere he / she has access to the Internet.

Many subscription services, such as Dropbox's paid business service, use advance methods to secure data through the use of multiple layers of security including, but potentially not limited to, SSL/TLS (Secure Sockets Layer / Transport Layer Security) for file sharing and the creation of a secure tunnel protected by 128-bit or higher AES encryption, and operating under the requirements of the ISO 27001 Certification in an effort to protect a user's data. Roughly translated, the service provider (in this example, Dropbox) creates a private tunnel through the internet between a user's computer and Dropbox's servers so that third parties cannot "see" the materials being transferred. Although file sharing service companies have their own controls and methods to transfer materials, the security provided by the file sharing service you choose may not meet your internal or your client's security requirements. As such, you should obtain an understanding of the type and extent of security utilized by third party providers when sharing/transferring/storing confidential materials. Be sure to choose a file sharing product or service that you can trust and that minimizes the risk(s) pertaining to the matter in which you are involved.

Recent security issues

It is common for file sharing sites to be on the defense from hackers attacking their Web sites to try to gain access to user information. Dropbox, Google Drive, and Box are just some of the commonly

Reprint with approval from the Kentucky CPA Journal



known file sharing services on the Internet today. This well-known status can lead to companies being frequently targeted by hackers from all over the world. This is another reason why some professional firms recommend clients use SFT protocol sites that can be trusted and that have been vetted to meet the firm's requirements.

Hackers attempting to access confidential information are a major concern to many professionals who use file sharing services and generally companies like Dropbox are on the forefront of keeping user information secure and safe. For example, Dropbox claims to block around 99 percent of hackers automatically, but even it admits that, "No company's code is perfect, and it's always far better for engineers to learn of and patch a security vulnerability before attackers are able to exploit it."

In May 2014, Dropbox made the public aware of "a Web vulnerability that impacted shared links to files containing hyperlinks." According to Dropbox, this issue affected many companies that utilized hyperlinks to access documents. The specific issue, according to Dropbox, was that under certain scenarios, "shared links to documents can be inadvertently disclosed to unintended recipients …" The unintended recipients could then use the link to access the information. As such, even though the materials are thought to be secure, the materials could have been accessed by an unauthorized person. If the materials accessed were confidential, this would cause some major concerns for all parties involved.

Further, in October 2014, Dropbox was in the news after being attacked by hackers who allegedly stole a variety of user names and passwords from other Web sites unrelated to Dropbox. The stolen credentials were then used to access secure content from a variety of third-party service providers, including Dropbox. Dropbox stated it had measures in place to detect suspicious login activity and it would automatically reset passwords when suspicious activity was identified.

After the October 2014 incident, Dropbox hired Ernst & Young LLP (E&Y) to perform a Service Organization Control 3 (SOC 3) examination. Under this examination, E&Y examined Dropbox's assertions that the Dropbox for Business System,

Continued on p. 26

Reprint with approval from the Kentucky CPA Journal

Security continued

during the period July 7, 2014 to Sept. 30, 2014:

- Was protected against unauthorized access, use or modification;
- Processing was complete, valid, accurate, timely, and authorized; and
- Information designated as confidential was protected as committed or agreed.

E&Y ultimately found that Dropbox's assertions were fairly stated.

Common prevention methods to help address the security dilemma

What can you do to better protect confidential client materials if the parties want to use a third-party supported file sharing service? Regardless of what is ultimately chosen to share /transfer client materials, it is recommended to always do the following:

- Understand the level of service you are receiving. Research the sharing service and understand what, if any, security and encryption is used by the service provider.
- Use a strong password - do not use the same password as you use for other websites and use a password with a mix of UPPER and lower case, $peci@l (special) characters, and Numb3r$ (numbers).
- Enable two-step verification, if available - a two-step verification will require a password and a security code (sent to another location like your personal e-mail or text message to your phone) to sign in.
- Actively monitor your account.
- Once documents have been successfully shared / transferred, or after an agreed upon period of time, remove the uploaded documents and / or disable the download link.
- Encrypt your files before uploading to a file sharing service provider. This adds another layer of security and many companies offer encryption services that are compatible with different cloud storage providers and platforms.

What should I do now?

It is strongly recommended for anyone to consider the security risks when transferring / storing confidential documents through a third party file sharing site. Reputable file sharing websites might be secure and safe enough for some users. However, if you do not know what the file sharing website's policy is regarding security, then be sure to find out before using it. Also, if the file sharing site is on top of their security, then it may meet or exceed your security requirements. Precautions should be taken (particularly for confidential information) and the appropriate due diligence should be performed in order to find a file sharing service that can be trusted and meets your security requirements.

About the authors: Alex Walther, CPA, CFE, David Kirk, CPA/CFF, and Ryan Broussard are members of Baker Tilly's National Forensic, Litigation & Valuation Services Group.

***Learn about security measures in the cloud**… register online at kycpa.org for KyCPA's CPAs in Business and Industry Conference, Sept. 17-18.*

Reprint with approval from the Kentucky CPA Journal